Amendments to the Specification

The following refers to the paragraph numbering used in the application as published.

Please replace paragraph [0004] with the following replacement paragraph:

[0004] To maintain the integrity of such transactions, it is necessary to implement a system in which the identity of the parties can be verified and for this purpose a number of signature protocols have been developed. Such protocols are based upon El Gamal signature protocols using the Diffie Hellman public key encryption scheme. One commonly used cryptographic scheme is that known as RSA but to obtain a secure transmission, a relatively large modulus must be used which increases the ~~band width~~ bandwidth and is generally undesirable where limited computing power is available. A more robust cryptographic scheme is that known as the elliptic curve cryptosystem (ECC) which may obtain comparable security to the RSA cryptosystems but with reduced ~~modulus~~ moduli.

Please replace paragraph [0011] with the following replacement paragraph:

[0011] In general terms, the present invention provides a method of ~~generating and verifying a signature between a pair of correspondents each of which shares a common secret integer comprising the steps of generating from a selected integer a session key at one of the correspondents, selecting a component of said session key and encrypting a message with said selected component, generating a hash of said selected component, and computing a signature component including said common secret integer, said hash and said selected integer and forwarding the signature component, encrypted message and has to the other correspondent. The selected integer may be recovered for the signature component using the common secret integer and the session key encrypted. The balance of the recovered session key may then be used to provide authorized and, optionally, a challenge to the recipient.~~ establishing a session key between a pair of correspondents in a data communication system, each of the correspondents sharing a secret information, the method comprising the steps of one of the correspondents generating an additional secret information and deriving therefrom a session key; the one of the

correspondents combining the secret information and the additional secret information in a signature algorithm to provide a first signature component; the one of the correspondents deriving a second signature component from the secret information; the one of the correspondents transferring the first and second signature components to the other of the correspondents; the other of the correspondents using the secret information to obtain the additional secret information from the first signature component and generating the session key from the secret information and the additional secret information; and the other of the correspondents verifying the second signature component by operating upon the session key obtained at the other of the correspondents to obtain a value corresponding to the second signature component and comparing such value with the second signature component.